

From: Ken McKinstry
To: HIPAA_Team; HIPAA_wkgrpc
Date: 1/16/01 5:30PM
Subject: HIPAA e-news

Some e-news, from HIPAALIVE mostly.
Ken

Various Meetings
Privacy & Security - Policies and Procedures

***** Various Meetings *****

The HIPAA Summit which is sponsoring the Second National HIPAA Summit, February 28-March 2, 2001 at The Marriott Wardman Park Hotel in Washington, D.C., see www.HIPAAsummit.com, is planning a HIPAA Summit West in Las Vegas or San Francisco in May or June.

WEDI/SNIP Conference 1/15- 1/17 Chicago, IL
WEDI Privacy PAG 2/26 - 2/27 in D.C. (same place as HIPAA II Conference)
HIPAA II conference 2/28-3/2
See www.wedi.org

There are two conferences coming up. AAHP in Washington DC starting on Feb. 27 and The 2nd National HIPAA Summit also in DC. Feb. 28-March 1.
website: www.hipaasummit.com

January 30 AFEHCT (Association For Electronic HealthCare Transactions) is sponsoring a meeting. The main topics of discussion will be the Privacy Final Rule and Vendor concerns. Visit the websites at www.afehct.org to register and for meeting information.

Additionally, the AFEHCT Annual Washington Policy Forum will be held in March. I'll get the dates and let you know.

***** Privacy & Security - Policies and Procedures *****

In organizations that I have been associated with they are separate and normally run by two different departments. Privacy policies are an extension of any records custodian policies, state and federal laws. This is usually because department heads are accountable and responsible for records their department maintains regardless of the media and who is maintaining it for them, ie IT. This also brings in data ownership and classification.

Security policies are the controls that are used against securing both non-sensitive and sensitive information. A baseline, security profile, requirements, etc. Good luck if you think it will only involve 10 or 20 pages. Policies need rationale statements (similar to the ones in the password policies in a earlier email), so that senior management and rank and file will understand the need to support them. Each policy topic needs guidelines, checklist, and easy understandable process document.

It is also a good idea to define the security and privacy role and its subprograms. For example:

Corporate Information Systems Security (CISS)

The CISS role and scope includes managing, consulting, and providing assistance to the following subprograms:

- a. Computer Security Policies and Standards. CISS is the corporate-level computer security policy-making organization responsible for the creation, evaluation, and administration of computer security policy, guidelines, and procedures in support of the organization security program.
- b. Security Certification and Accreditation Program. A system must be secured at a level appropriate to its value to the [organization] or because of statutory requirements. The security level is based on a determination of sensitivity and criticality made by the owner, by classifying the information to be processed and evaluating whether the application is a major system and critical to the [organization] operation. The executive owner of a system is responsible for ensuring that security issues are considered in the early phases of system development.
- c. Access Control and Management. Access to systems, data, and information must be controlled and secured at a level appropriate to their value. This is the responsibility of all employees and contractors. Systems and information must be managed and secured to provide protection both to the [corporation] and to the users of the systems. The degree of protection is dependent on management categorization of the sensitivity of information processed and the criticality of these systems.
- d. Network Security. A telecommunications network must be secured at a level appropriate to its value to the [corporation] or because of statutory requirements. It must also be reliable and available for use by the [corporation]. CISS provides consulting, monitoring, and support for the postal network. These activities include evaluating firewalls, providing encryption solutions, and reviewing business partner connectivity and WEB servers.
- e. Contingency Planning. All applications defined by executive sponsors (or users' managers for local systems) as critical to their operations, must be supported by an up-to-date, tested contingency plan. CISS provides consulting support in this area.
- f. Risk Management. All corporate managers must assess the vulnerabilities and risks of both automated systems and sites in order to develop and implement cost-effective security measures. CISS consults and provides overall [corporation] policy on this program.
- g. Computer Security Awareness. All employees must have awareness of their computer security responsibilities relative to the use of computers, automated systems, and information being processed. This includes the safeguarding of their logon IDs and passwords, the physical security of computer equipment, and the protection of sensitive information. CISS manages the security awareness program.
- h. Computer Security Technology Assessment. The [corporation] must keep abreast of the changing computer security technology and make recommendations for the deployment of the new technology in a responsible manner. CISS evaluates and recommends security products for implementation.
- i. Personal Computers, Local Area Networks (LAN), and General Support Systems. A security program has been implemented that provides basic security protection for personal computers, LAN(s), and general support systems at a level appropriate to their value to the [corporation] or because of statutory requirements. CISS provides guidelines and policy to support this program.
- j. Security Architecture. Security architecture is required to protect [corporation] information processing systems containing sensitive information. CISS is responsible for managing and developing this architecture.
- k. Personnel Security. Clearances must be obtained for persons in sensitive positions. Management's responsibility is to ensure that data processing-related positions meet the security guidelines established by the [corporation] and that all information systems-related positions requiring sensitive clearances are identified and that clearances are kept current.
- l. Physical Security. Computer equipment, data, facilities, and information must be safeguarded at a level appropriate to their value to the [corporation] or because of statutory requirements. The facilities security officers, who are not to be confused with an information systems security officer, are responsible for both facility physical security and personnel security. Due to a potential conflict of interest, individuals cannot be assigned both duties. CISS and Facility security must work closely with each other to ensure both the protection of individual and their privacy of information.
- m. Computer Security Audit, Evaluation, and Review. The Office of Audit is responsible for auditing [corporate] information systems and performs developmental audits of automated systems, audits of

operational and financial systems, and environmental audits. CISS performs operational security compliance reviews of computer systems and/or computer sites. CISS will provide audit and other support to the Office of Audit, as required.

Privacy Acts Officer (PAO)

The PAO assists department records custodians, who are also the owners of the applications, to determine the sensitivity of their information and to comply with the Privacy Act when that Act applies. Under the category of Automated Information Processing Security, all information maintained on information processing equipment requires protection. Sensitive information requires a greater degree of protection. Departmental heads must evaluate the information they intend to maintain on information processing equipment for its sensitivity. Security measures must also be in place to protect all sensitive information. The PAO officer provides assistance on the proper information classification and Privacy Act.

TESS @1999

remember these are just more management opportunities - have fun.

Walter S. Kobus, Jr., CISSP, MSTI
